

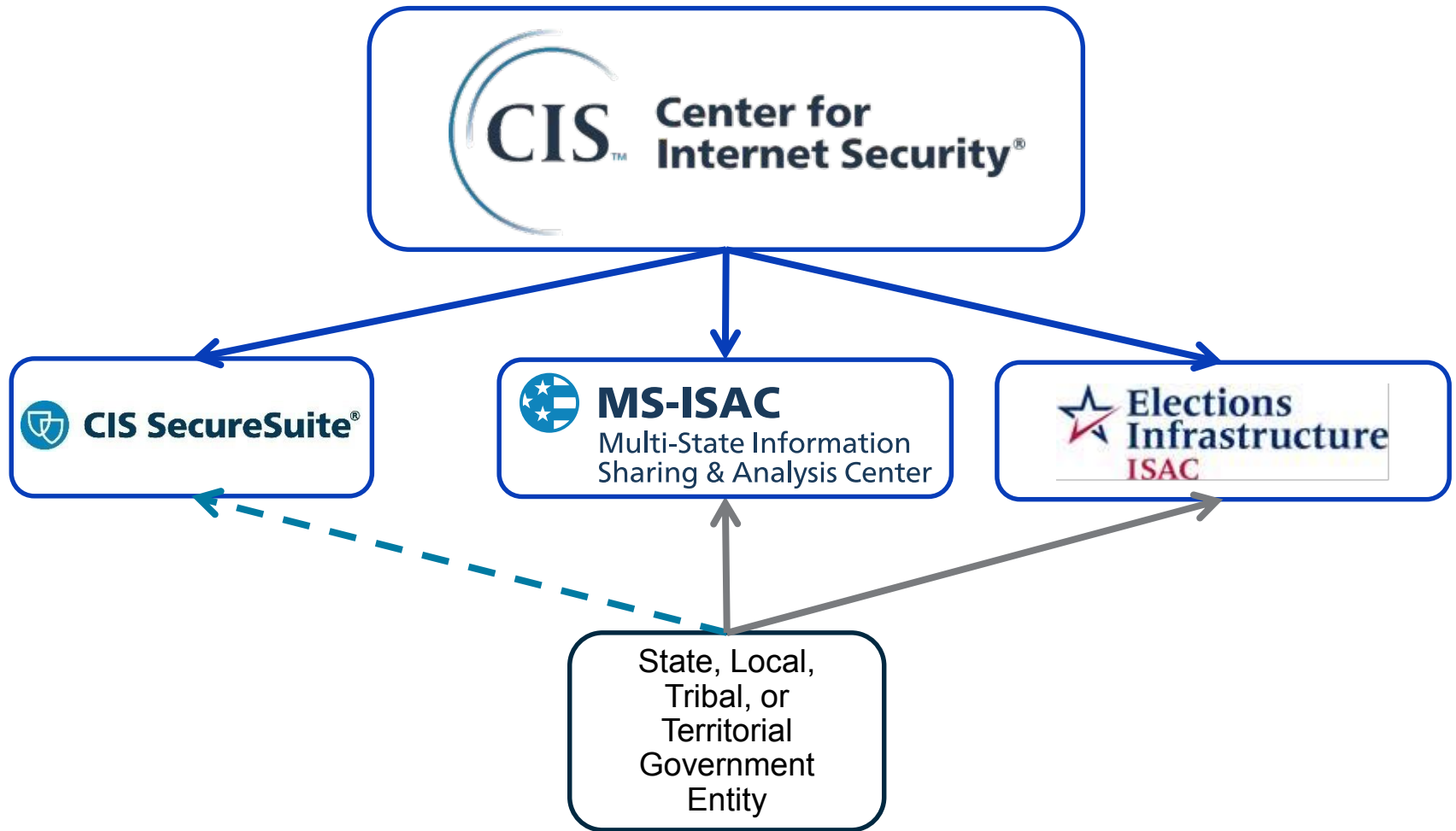


MS-ISAC Services

Cybersecurity Best Practices and Free Resources

Kateri Gill

May 24, 2018





Who We Serve

MS-ISAC Members include:

- All 56 US States and Territories
- All 79 federally recognized fusion centers
- More than 2,800 local governments and tribal nations
 - More than 200 in Texas

State, Local, Tribal, and Territorial

Cities, counties, towns, airports, public education, police departments, ports, transit associations, and more



About MS-ISAC Membership

Free and Voluntary

No Mandated Information Sharing

One Form to Complete

To join or get more information:

<https://learn.cisecurity.org/ms-isac-registration>



24 x 7 Security Operations Center

Central location to report any cybersecurity incident

- **Support:**
 - Network Monitoring Services
 - Research and Analysis
- **Analysis and Monitoring:**
 - Threats
 - Vulnerabilities
 - Attacks
- **Reporting:**
 - Cyber Alerts & Advisories
 - Web Defacements
 - Account Compromises
 - Hacktivist Notifications



To report an incident or request assistance:

Phone: 1-866-787-4722

Email: soc@msisac.org



Create an Incident Response Playbook

Best Practice



Incident Response Planning

MS-ISAC Cyber Incident Response Guide Recommended Resources

Incident Response

- Defining Incident Management Processes: A Work in Progress (www.cert.org/archives/pdf/08tr015.pdf)
- CERT/CC, Avoiding the Trial-by-Fire Approach to Security Incidents (http://www.sei.cmu.edu/news-at-sei/columns/security_matters/1999/mar/security_matters.htm)
- NIST SP-800-86 "Guide to Integrating Forensic Techniques into Incident Response"
- National Information Assurance (IA) Approach to Incident Management (IIM) (<http://www.ciss.gov/Assets/pdf/1/NIS-048-07.pdf>)

Incident Reporting

- NIST SP 800-61 (<http://csrc.nist.gov>)
- NIST SP-800-91 "Incident Management"
- ([https://buildsecuritypractices/incident/](https://buildsecurityinto.usability.gov/buildsecuritypractices/incident/))

Incident Detection

- IP-CERT: Cymru

Business Impact Analysis (BIA) Guide

Published _____, 2017

Step one of the BIA process: determine function and system criticality

Working with input from users, managers, mission/business process owners, and other internal or external points of contact (POC), identify the specific mission/business processes that depend on or support the information system.

Mission/Business Process	Description
Provide emergency response	Essential Function to provide emergency services, police, fire, EMS to the community.
	Process of obligating funds, issuing check or electronic payment and acknowledgment receipt

Business Impact Analysis Planning Process

```
graph LR; A[US Labor Code] --> B[Admin Code]; A --> C[Vernon's Civil Statute]; A --> D[Government Code]; B --> E[Occupations Code]; B --> F[Other Code]; E --> G[Identify Agency Statutory Requirements]; F --> G; G --> H[Vision & Mission]
```

To-Go Kit Contents a/k/a To-Go Kit / Take-away Kit / Tool Kit / Bug-out Bag

- Directions to alternate site
- Instructions – specific to alternate site, etc.

site – Security, key(s), Facility personnel, contact info for POC

has an active land line(s)

oper ID

spot, adapters

nuity/Disaster Recovery/COOP Plan (hardcopy if reasonable is size, on a CD/USB

Hot Wash How-To

Published Fall, 2017

What is a Hot Wash?

A "Hot Wash" is a post-action review completed ideally within 24 hours of an incident or exercise (or as soon as practical) to identify strengths and weaknesses of the response effort, to verify that response and recovery goals are met, to evaluate training and staff

MS-ISAC™
Multi-State Information
Sharing & Analysis Center®



Computer Emergency Response Team

- Incident Response (includes on-site assistance)
- Network & Web Application Vulnerability Assessments
- Malware Analysis
- Computer & Network Forensics
- Log Analysis
- Statistical Data Analysis

To report an incident or request assistance:

Phone: 1-866-787-4722

Email: soc@msisac.org



After Action Review

- Who, What, Why, Where and How it Happened
- The Good, The Bad, and The Ugly
- Incident Response Plan
- Training
- Documentation





Back Up Your Data

Best Practice



National Webcasts

A collaborative effort between DHS and MS-ISAC to provide timely and relevant cybersecurity education and information

- The Working Cloud: Tackling the Security Risks (June 22, 2017)
- The Expanding Attack Surface (April 2017)
- Cybersecurity While Traveling (February 2017)
- Cybersecurity Year in Review and 2017 Preview (December 2016)
- National Cybersecurity Awareness Month – Be a Part of Something Big (October 2016)
- State and Local Roundtable – Effective Cyber Disruption Strategies (August 2016)

<https://msisac.cisecurity.org/webcast/>



Cyber Exercises

September 2017 Scenario

Last year your organization had a server crash and lost a large amount of data which required you to update your incident response procedures once again, and you lost a large sum of data. During last year's lessons learned recovery process left out some key data loss. Unfortunately, the recovery process was not updated to address this outcome.

Discussion

NIST Functions Addressed: **PR.IP-10:** Response and recovery plans are tested; **RS.IM-1:** Response plans incorporate lessons learned; **RS.IM-2:** Response strategies are updated; **RC.IM-1:** Recovery plans incorporate lessons learned; **RC.IM-2:** Recovery strategies are updated

- Who would be responsible for updating the response plans and recovery strategies?
- Do you have procedures outlining how to complete an after action report?
 - What methods do you use within your organization in order to ensure deliverables from your hotwash are completed?
- Do your change management processes include guidance for updating these procedures?
- Who is responsible for testing your response plans?
 - Do you run separate tests after updates are made?
- Have you referenced the MS-ISAC's "How to Hotwash" document on the HSIN Portal?



Update Your Software and Systems

Best Practice



MS-ISAC Advisories



chrome



ANDROID



TLP: WHITE

... was sent with High importance.
From: MS-ISAC Advisory
To: Thomas Duffy
Cc:
Subject: MS-ISAC CYBER SECURITY ADVISORY - Multiple Vulnerabilities in Adobe Flash Player Could Allow for Remote Code Execution

MS-ISAC ADVISORY NUMBER:
2015-119 - UPDATED

DATE(S) ISSUED:
10/13/2015
10/15/2015 - Updated

SUBJECT:
Multiple Vulnerabilities in Adobe Flash Player Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities in Adobe Flash Player could allow remote code execution. An attacker could exploit these vulnerabilities to cause a user's computer to perform actions without the user's knowledge or consent, such as displaying pop-up windows, downloading files, or transmitting confidential data, compromising processing resources in a user's computer, or remotely controlling the user's computer.

THREAT INTELLIGENCE
There are currently no reports of these vulnerabilities being exploited in the wild.

October 15 - UPDATED THREAT INTELLIGENCE
Adobe is aware of a report that an exploit for the CVE-2015-7645 critical vulnerability was used in the wild.

- March 2017
- #2017-028 » Thursday, March 16, 2017
[Multiple Vulnerabilities in Drupal Could Allow for Remote Code Execution](#)
 - #2017-027 » Tuesday, March 14, 2017
[Multiple Vulnerabilities in Microsoft Office Could Allow for Remote Code Execution \(MS17-014\)](#)
 - #2017-026 » Tuesday, March 14, 2017
[Multiple Vulnerabilities in Microsoft Graphics Component Could Allow for Remote Code Execution \(MS17-013\)](#)
 - #2017-025 » Tuesday, March 14, 2017
[Multiple Vulnerabilities in Microsoft Uniscribe Could Allow for Remote Code Execution \(MS17-011\)](#)
 - #2017-024 » Tuesday, March 14, 2017
[Multiple Vulnerabilities in Microsoft Windows SMB Server Could Allow for Remote Code Execution \(MS17-010\)](#)
 - #2017-023 » Tuesday, March 14, 2017
[A Vulnerability in Microsoft Windows PDF Library Could Allow for Remote Code Execution \(MS17-009\)](#)
 - #2017-022 » Tuesday, March 14, 2017
[Cumulative Security Update for Microsoft Edge \(MS17-007\)](#)
 - #2017-021 » Tuesday, March 14, 2017
[Cumulative Security Update for Internet Explorer \(MS17-006\)](#)
 - #2017-020 » Tuesday, March 14, 2017
[Multiple Vulnerabilities in Adobe Flash Player Could Allow for Code Execution \(APSB17-07\)](#)
 - #2017-019 » Friday, March 10, 2017
[Multiple Vulnerabilities in Google Chrome Could Allow for Remote Code Execution](#)
 - #2017-018 » Thursday, March 09, 2017
[Vulnerability in Apache Struts Could Allow for Remote Code Execution](#)
 - #2017-017 » Wednesday, March 08, 2017
[Multiple Vulnerabilities in Mozilla Firefox Could Allow for Arbitrary Code Execution](#)
 - #2017-016 » Monday, March 06, 2017
[Multiple Vulnerabilities in Google Android OS Could Allow for Remote Code Execution](#)
 - #2017-015 » Monday, February 27, 2017
[Vulnerability in Microsoft Internet Explorer and Edge Could Allow for Arbitrary Code Execution](#)



Monitoring of IP Range & Domain Space

IP Monitoring

- IPs connecting to malicious C&Cs
- Compromised IPs
- Indicators of compromise from the MS-ISAC network monitoring (Albert)
- Notifications from Spamhaus

Domain Monitoring

- Notifications on compromised user credentials, open source and third party information
- Vulnerability Management Program (VMP)

Send domains, IP ranges,
and contact info to:
soc@msisac.org



Vulnerability Management Program

Web Profiler

What Data Are We Collecting?

- Server type and version (IIS, Apache, etc.)
- Web programming language and version (PHP, ASP, etc.)
- Content Management System and version (WordPress, Joomla, Drupal, etc.)

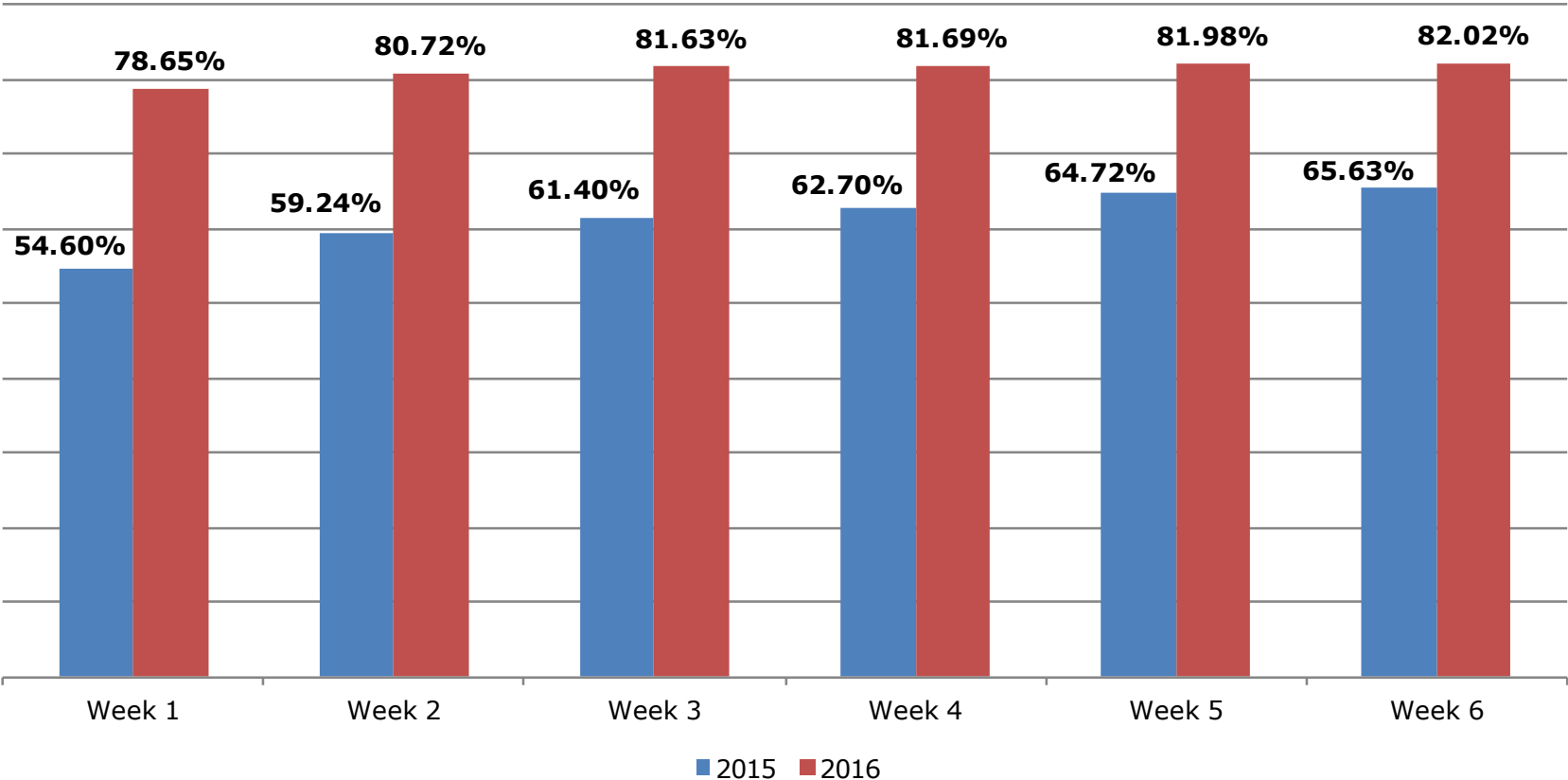
Email notifications are sent with 2 attachments containing information on out-of-date and up-to-date systems:

- Out-of-Date systems should be patched/updated and could potentially have a vulnerability associated with it
- Up-to-Date systems have the most current patches



Time-to-Patch

% of Patched Word Press Instances Following A New Version



Train Your End Users

Best Practice

<https://www.youtube.com/watch?v=opRMrEfAlil>




Monthly Newsletter

Distributed in template form to allow for re-branding and redistribution by your agency

March, 2017
Volume 12, Issue 3

Common IT Wisdom That Keeps You Secure

**MS-ISAC**
Multi-State Information
Sharing & Analysis Center

Insert your agency name and contact info
here

From the Desk of Thomas F. Duffy, Chair, MS-ISAC

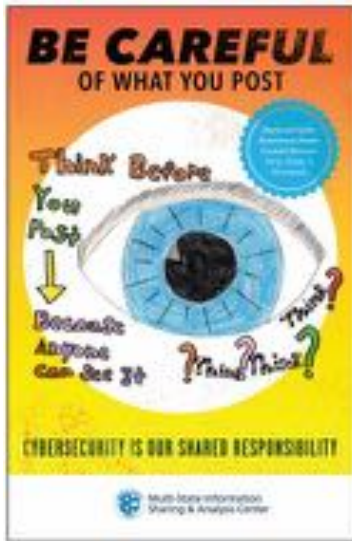
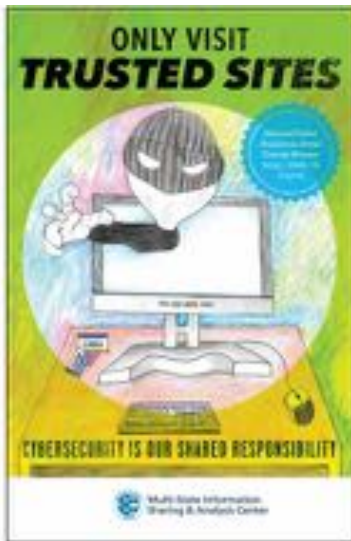
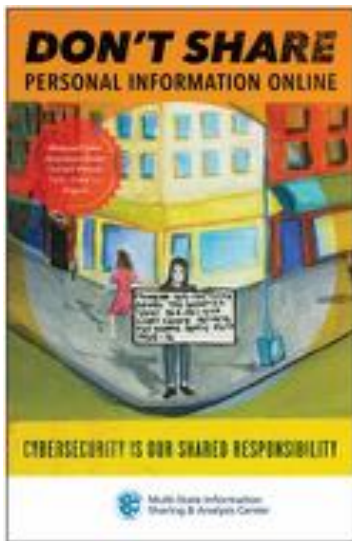
Day in and day out, employees hear the same things from their IT staff about cybersecurity and safety. Though they may sound like a broken record, there are very important reasons and rationale behind these practices and advice. Keeping safe and secure while connected isn't just about how your system is set up - it is also very much about how you end up using it. Below, we discuss some common IT staff wisdom and provide some background information and the rationale as to why it definitely merits your attention.

Make sure you lock your screen when you are away from your desk.

Screen locking policies exist for a reason. Even if you are leaving for just a few minutes at a time, be sure to lock your screen. Though physical intruders are rare during daytime and in conventionally secured offices, intrusions do occasionally happen. Screen locks also thwart opportunistic insider attacks from other employees that may seek to obtain information or access information beyond what they should normally have. If you don't adhere to a screen locking policy, an attacker can simply walk up and start manipulating or stealing your



Cybersecurity Awareness Toolkit





EI-ISAC Awareness Products



Denial of Service (DoS) Attacks

What it is: A denial of service attack (DoS) is a cyber attack that originates from a singular source and seeks to disrupt the availability of a system or service. Typically, these attacks target web servers in order to overwhelm the webserver's Internet connection or its ability to respond to user requests. If the attacker can send more requests than permitted by the system, the webserver or Internet connection will be too busy to respond to additional requests, resulting in a "denial of service" to legitimate users until the number of requests returns to normal levels. To increase effectiveness, attackers may use multiple source computers in a distributed denial of service (DDoS) attack. Of note, computers participating in a DDoS attack may be infected with malware that conducts the attack, which means they are also victims of malicious activity.

Why does it matter: Attacks like this could be the result of a politically motivated actor targeting the elections infrastructure or elections infrastructure may be indirectly impacted by targeting against other state/county/city infrastructure. DoS attacks can also be accidental in time. A well-timed DoS attack near a candidate accessing online services and/or websites, resulting in a denial of service.

TLP: WHITE MS-ISAC Elections Pilot Weekly News Alert

TO: All MS-ISAC Elections Community Members

DATE: January 17, 2018

SUBJECT: Elections Pilot Weekly News Alert 1/17/18

The MS-ISAC Elections Pilot Weekly News Alert is a summary of open-source reporting on election security and topics that may be of interest to elections officials. The Weekly News Alert is intended to provide situational awareness of cyber risk landscape and cybersecurity best practices to election officials through open source news reporting and analysis by the MS-ISAC and other experts. If you would like to submit security-related stories that may be of interest to the elections community, please contact ben.spear@cisecurity.org

Senate Bill Seeks Consequences for Future Election Interference - The Hill (1/16/18, 1/12/18)

On January 16, 2017, Senators Marco Rubio and Chris Van Hollen introduced the "Defending Elections from Threats by Establishing Roadlines (DETER) Act," which lays out what specific activities to subvert U.S. elections would merit a federal response. The legislation would require the Administration to provide to Congress, within 90 days of enactment, plans to counter potential election interference from specific countries identified as a threat, and a notification to Congress of any foreign election interference within one month after every federal election. The bill also spells out specific penalties for future interference by Russia, such as a requirement to blacklist political figures and impose sanctions on Russia's finance, energy, and defense sectors.

MS-ISAC Analyst Note: The DETER Act acknowledges that nation-state actors are a persistent threat that will continue to target a range of U.S. interests and adds to the

Products that put elections security topics into context for both technical and executive staff



FedVTE

Free Online Training Environment

- CompTIA A+, Network+, Security+
- CISSP Certification Prep
- Operating System Security

www.fedvte.usalearning.gov



Request Account

Request an access email here.





Be Wary of Phishing

Best Practice



Malicious Code Analysis Platform

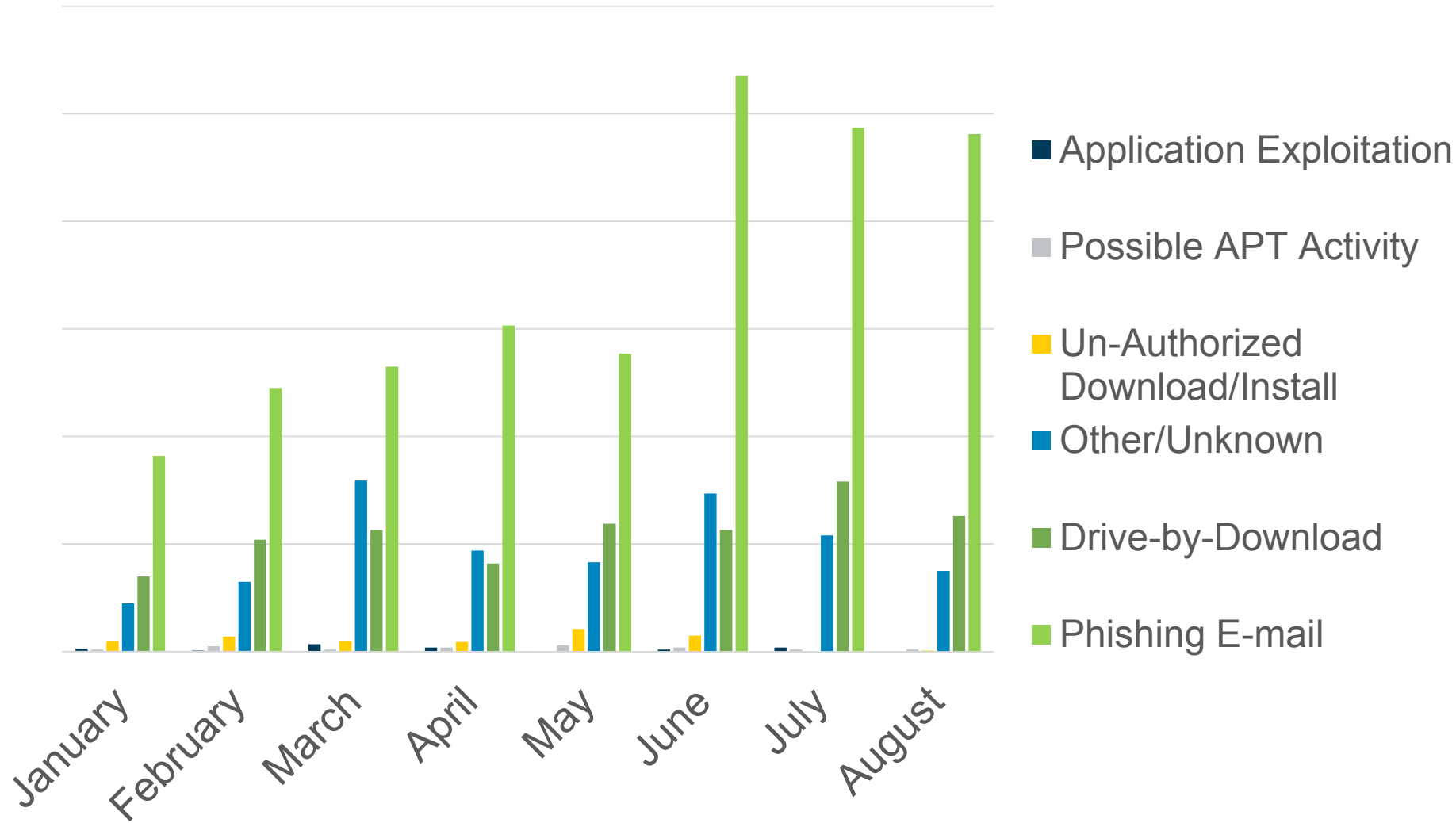
A web based service that enables members to submit and analyze suspicious files in a controlled and non-public fashion

- Executables
- DLLs
- Documents
- Quarantine files
- Archives

To gain an account contact:
soc@msisac.org



MCAP Malware Sources By Month





Ukraine's Critical Infrastructure - 2015

- Boryspil International Airport – Kiev, Ukraine
- Power Grid Shut Down
- 80,000 customers lost power for 6 hours
- BlackEnergy Malware
- Attributed to Russia





MS-ISAC Cyber Alerts

MS-ISAC Advisory

Sent: Thursday, June 16, 2016 at 2:57 PM

To: Thomas Duffy

TLP: WHITE
MS-ISAC CYBER ALERT

TO: All MS-ISAC Members, Fusion Centers, and IIC partners

DATE ISSUED: June 16, 2016

SUBJECT: Malicious Email Campaign Targeting Attorneys Spoofs Emails From Statewide Legal Organizations - TLP: WHITE

In June 2016 MS-ISAC became aware of a malicious email campaign targeting attorneys, which spoofs emails from statewide legal organizations, such as the Bar Association and the Board of Bar Examiners. The subject and body of the emails include claims that "a complaint was filed against your law practice" or that "records indicate your membership dues are past due." Recipients are asked to respond to the claims by clicking a link which leads to a malicious download, potentially ransomware.

The emails are well written and appear to originate from the appropriate authority, such as an Association official, likely increasing their effectiveness. Reporting from various states indicates a likelihood that this campaign is personalized to individuals practicing in a particular state and may be progressing on a state-by-state basis. The following states have been referenced in public reporting on this campaign: Alabama, California, Florida, Georgia, and Nevada. This targeting may include attorneys working for state, local, tribal, and territorial (SLTT) governments.

Recommendations:

MS-ISAC recommends the following actions:

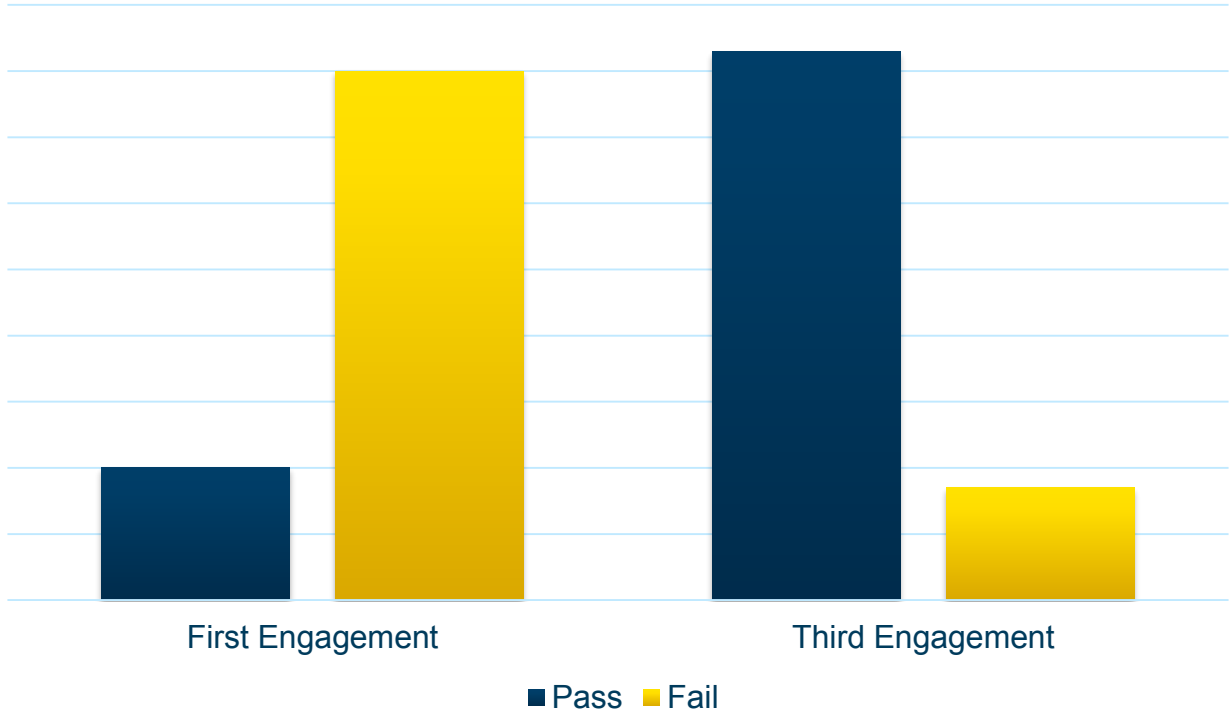
- Share this information with potentially impacted organizations your area of responsibility, including Departments of Law/Justice, related law enforcement agencies, and agency-specific offices of counsel.
- Train government legal professionals in identifying spear phishing emails which may include spoofed email addresses, unusual requests, and questionable and/or masked links. This particular series of emails includes what appears to be a link to the state bar association, but when the user hovers over the link it shows that the link is really to a different website. Copying and pasting the link, instead of clicking on it, would defeat this social engineering attempt.
- Perform regular backups of all systems to limit the impact of data loss from ransomware infections. Backups should be stored offline.

TLP: WHITE



Phishing Engagements

Case Study: MS-ISAC Member



Failure Rate is Equal to Percentage of Users Who Clicked the Provided Link



Involve Executives in Cybersecurity

Best Practice



MS-ISAC Annual Meeting

2017-2018 Annual Meeting

New Orleans, Louisiana

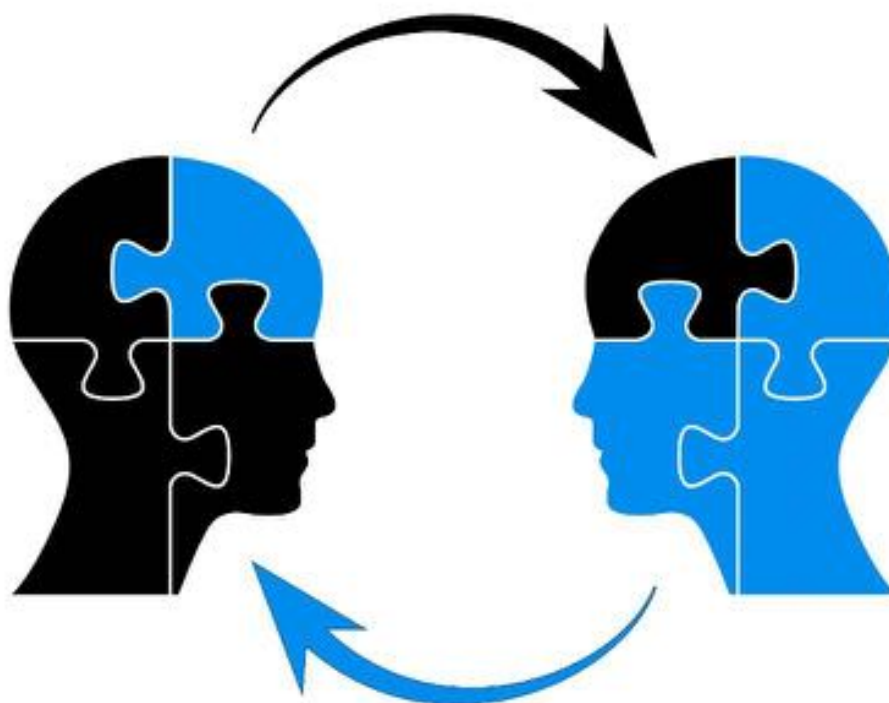
April 9-11, 2018





MS-ISAC Mentoring Workgroup

Open call for members every November





Employ a risk-based approach to security

Best Practice

Classic Risk Equation

$$\text{Risk} = f \left\{ \frac{\text{Vulnerability, Threat, Consequence}}{\text{controls}} \right\}$$



Weekly Malware IPs and Domains

Automated Threat Indicator Sharing via Anomali

From: MS-ISAC SOC
To: MS-ISAC SOC
Cc:
Subject: Message from the MS-ISAC: Malware IPs and Domains observed by MS-ISAC 11/23/2019

Message: IPs of Interest 11-23 to 11-29.xlsx (35 KB)

Attached to this email is a list of IP addresses and domains associated with malware.

Recipients may only share TLP: GREEN information with peers and partner organizations within their sector or community.

This list is produced from data collected by the MS-ISAC. Currently this data is being collected across a number of States and Local Governments.

The spreadsheet contains four tabs with the following information:

1. Malware IP Data

IP Address – This is either the IP address that is attacking a system or the IP address malware on an infected system is communicating with.

Counts – This is the number of alerts generated for malicious traffic to or from the IP address.

Country, Region, City – Location of the potentially malicious IP address.

IP ADDRESS	LOG COUNT	EVENT COUNT	COUNTRY	ASSOCIATED THREAT
69.162.1.108	1522		United States	Luminosity, LuminosityLink
14.67.112.248	969		United States	Luminosity
18.141.44.145	143		Netherlands	Generic Trojan
44.145	83		United States	Floerchvet
44.165	23		Germany	Ursnif
1.125.32	13		United States	Various malware, WS/S Downloader
149.172	10		United States	Various malware, WS/S Downloader
	7		United States	Various malware, WS/S Downloader
	4		United States	Kovter
			United States	Cerber



To gain an Anomali account contact:
Indicator.sharing@msisac.org

TLP: WHITE



Vulnerability Management Program

Port Profiler

- **12 common ports – services identified by reading banner information**
 - Services: FTP, SSH, HTTP(S), SMB, RDP, VNC, SQL, and MongoDB
- **Quarterly notifications**
- **Contact**
vmp.dl@cisecurity.org to:
 - Opt out of this service
- **Source IP address:**
52.14.79.150

IP Address	Hostname	Port	Service	Tag	Banner
152.168.1.111	host-111.test.com	443	HTTPS	Screen	Apache Tomcat/7.0.89
152.168.1.124	tep.test.com	80	HTTP	Screen	IS Windows Server
152.168.1.123	my.test.com	80	HTTP	Screen	IS Windows Server
10.11.12.4	pm01.ne.test.com	21	FTP	Printer	220 FTP print service/V-1.13/Use the network password for the ID if updating /r/r/n
10.11.12.7	rcp.ne.test.com	23	TELNET	Printer	!!!vR/COH Maintenance Shell. !!!vR/COH User access verification.!!!vR/login:
10.11.12.53	350cam.cmc.test.com	21	FTP	Other	220 AXIS 210A Network Camera 4.40.1 (Sep 11 2007) ready/r/n
10.11.12.50	Could Not Resolve	21	FTP	Other	220 Welcome to the Cisco TelePresence MCU 4505, version 4.3(2.18)/r/n
10.11.12.199	switch.test.com	80	HTTP	Networking	/r/n /r/n ProCurve Switch 2810-48G (J9022A)/r/n
10.11.12.7	rcp.ne.test.com	8080	HTTP	-	404 Not Found
10.11.12.199	switch.test.com	23	TELNET	-	!!!vR/COH Sorry, the maximum number of telnet sessions are active. Try again later.!!!vR/COH





- MS-ISAC Cyber Alert Map
- Archived webcasts & products
- Cyber table top exercises
- Guides and templates
- Message boards





MS-ISAC Intel Papers

UNCLASSIFIED//FOR OFFICIAL USE ONLY • Traffic Light Protocol: **GREEN**

Multi State Information Sharing and Analysis Center Cyber Monthly Update

Information current as of May 31, 2017



TLP: WHITE



TECH
WHITE
February

Timely Patching Reduces System Compromises

Authored by: Katelyn Bailey, Cyber Intel Analyst

INTRODUCTION

Patching and updating systems is one of the most important cyber security practices to implement in order to protect a system from being compromised. Analysis of information shared by the Multi-State Information Sharing and Analysis Center (MS-ISAC) data proves that timely patching can prevent most infections and system compromises.

DETAILS

Patches and security updates address software vulnerabilities that may allow malicious cyber threat actors access to information systems or a network. Once vulnerabilities are publicly announced, the information is available to anyone, including cyber threat actors. It is essential to quickly patch vulnerable systems as the disclosed information makes it easier for cyber threat actors to find and target systems. Research has shown that despite the proven effectiveness of patching, systems often remain vulnerable with out-of-date software and plugins for extended periods.

In July 2015 cyber threat actors exfiltrated data from an Italian company, which included information on four zero-day exploits that targeted vulnerabilities in common software. The Angler Exploit Kit, which dropped both the CrymWall and Kovter malware in July 2015.

The primary vector in at least the incidents investigated by MS-ISAC was an unpatched vulnerability in an operating system, software, or plugin.

UNCLASSIFIED//FOR OFFICIAL USE ONLY • TLP: **AMBER**

Situational Awareness Report

This proprietary document is based on the February 2017 security event data.



Multi-State Information Sharing and Analysis Center

UNCLASSIFIED//FOR OFFICIAL USE ONLY • TLP: **AMBER**



MS-ISAC Security Primer Cybersecurity While Traveling

March 2017, SP2017-0817

OVERVIEW: Whether you are traveling for business or leisure, travelers face increased cyber targeting and key threats include accidental loss and exposure, financially-motivated crime, data; oversampling information; the information carried with the traveler; the traveler's family; and the lack of due diligence. The Multi-State Information Sharing and Analysis Center (MS-ISAC) recommends assessing travel risk based on the threats and gaps in your knowledge.

When traveling for business or leisure, travelers face increased cyber targeting and key threats include accidental loss and exposure, financially-motivated crime, data; oversampling information; the information carried with the traveler; the traveler's family; and the lack of due diligence. The Multi-State Information Sharing and Analysis Center (MS-ISAC) recommends assessing travel risk based on the threats and gaps in your knowledge.

MSIS:

When traveling for business or leisure, travelers face increased cyber targeting and key threats include accidental loss and exposure, financially-motivated crime, data; oversampling information; the information carried with the traveler; the traveler's family; and the lack of due diligence. The Multi-State Information Sharing and Analysis Center (MS-ISAC) recommends assessing travel risk based on the threats and gaps in your knowledge.

When traveling for business or leisure, travelers face increased cyber targeting and key threats include accidental loss and exposure, financially-motivated crime, data; oversampling information; the information carried with the traveler; the traveler's family; and the lack of due diligence. The Multi-State Information Sharing and Analysis Center (MS-ISAC) recommends assessing travel risk based on the threats and gaps in your knowledge.

UNCLASSIFIED//FOR OFFICIAL USE ONLY • Traffic Light Protocol: **AMBER**

DESK REFERENCE

Cyber Threat Actor Review

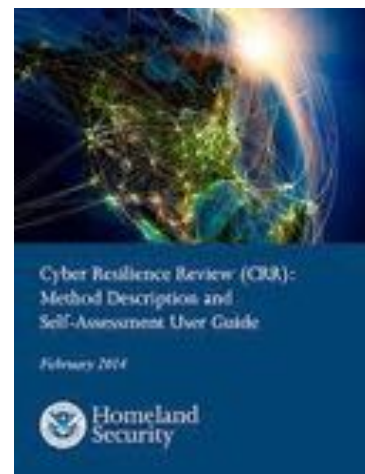
Information from October 1 to December 31, 2015

(U) TLP: **AMBER** This desk reference provides a review of the most active, identified¹ Cyber Threat Actors^{2,3} (CTA) and malicious cyber campaigns and operations from October 1 through December 31, 2015. The information in this document is provided to further the reader's



Cyber Resilience Review (CRR)

- **Self-Assessment or In-Person Interview**
 - No Cost
 - Based on the Cyber Resilience Evaluation Method and the CERT-RMM



www.dhs.gov/cyber



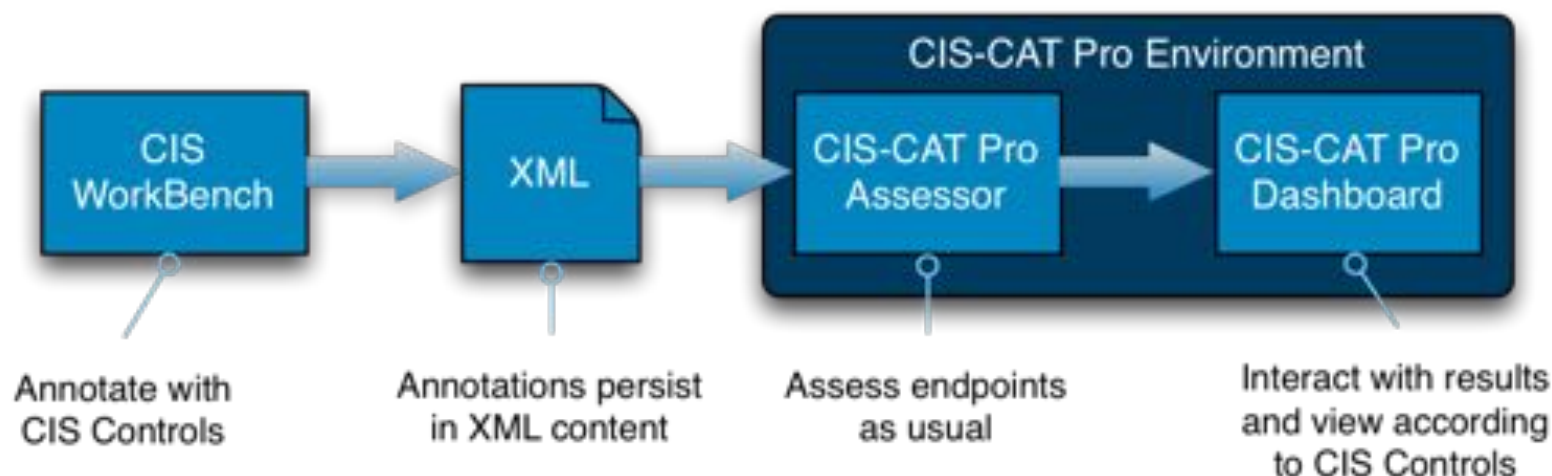
SecureSuite

- **Workbench**

- Platform for creating and maintaining resources
- <https://workbench.cisecurity.org>

- **CIS-CAT Pro**

- Configuration and Vulnerability Assessment Tool
- Assessor and Dashboard can be downloaded from Workbench





Cybersecurity Best Practices

- Create an Incident Response Playbook
- Back up your Data
- Update Your Software and Systems
- Train your End Users
- Be Wary of Phishing
- Involve Executives
- Take a Risk-Based Approach

Questions?





MS-ISAC 24x7 Security Operations Center

1-866-787-4722

SOC@cisecurity.org

<https://learn.cisecurity.org/ms-isac-registration>

Kateri Gill

Senior Program Specialist

518-880-0779

Kateri.Gill@cisecurity.org